UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

In the matter of the Search of

INFORMATION THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE, 1600 AMPITHEATRE PARKWAY, MOUNTAINVIEW, CALIFORNIA 94043

Case No. 22-MR-633
Filed Under Seal

GOOGLE LLC'S MOTION TO QUASH SEARCH WARRANT AND BRIEF IN SUPPORT THEREOF

INTRODUCTION

This Motion to Quash involves what is commonly referred to as a "geofence" search warrant. The warrant directs Google to search the Location History data of all of its users and disclose information about any users for whom a stored Location History data point falls within one of the three specified search areas. Each of the three search areas is defined as a 300-meter radius around a central point in Santa Fe, New Mexico. The combined search areas encompass over 200 acres. The search periods span between 10 minutes and 24 minutes for a combined search time of 44 minutes. The search encompasses, among other things: at least 20 medical offices, including a portion of the St. Vincent Pediatrics building; a number of pharmacies; at least two law firms; a church; a large and popular hotel (the Residence Inn by Marriott Santa Fe); more than 100 homes and a number of apartment complexes; a branch office of the Department of Motor Vehicles; a portion of an elementary school parking lot; a heavily trafficked seven-lane road (St. Michael's Drive); a portion of a Highway 285 off-ramp; and numerous stores, banks, restaurants, and other commercial establishments. Although the search seeks evidence regarding the commission of a crime by an individual or small number of individuals, *the search yields nearly 450 devices.*

The search authorized by the warrant sweeps in the data of hundreds of individuals who may have been enjoying the privacy of their homes, sitting with their sick children at the doctor's office or attending their own medical appointments, picking up medicine from or seeking the advice of a pharmacist, consulting with their lawyer, praying, eating at a restaurant during their lunch hour, or engaging in any number of other activities entirely unrelated to the crimes under investigation. The warrant is a modern-day, digital equivalent of a general search and must be quashed.

BACKGROUND

I. Geofence Warrants and Google's Location History Service

A. Geofence warrants

Search warrants issued pursuant to the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.*, frequently compel service providers such as Google to disclose stored communications content or records "pertaining to a subscriber to or customer of such service," including data that reveals those persons' locations and movements at particular times of interest. *Id.* § 2703(c). So-called geofence warrants take a different approach. Rather than direct Google to disclose the records or information pertaining to a particular customer or customers, they direct Google to identify all Location History users whose data suggests they were in a given area during a given time frame—personal information the Government will then sort through in an attempt to identify a person of interest. To comply with a geofence warrant, Google must search all users' Location History to determine if any stored Location History is consistent with the warrant's search

parameters. Declaration of Marlo McGriff In Support of Motion to Quash ("McGriff Decl."), ¶ 16, filed contemporaneously herewith and incorporated herein by reference.

B. Google's Location History service

Location History is an optional service, available only to Google Account holders, that is not activated by default. *Id.* ¶ 4. For Location History to function—and for the service to store information regarding a user's location—the user must take several affirmative steps. *Id.* ¶ 7. *First*, the user must ensure that the device-level location setting on their mobile device is turned on. *Id.* When the device-location setting is activated, the mobile device automatically detects location based on a combination of inputs, including GPS signals, Wi-Fi connections, and cellular networks.[1] *Id. Second*, for those devices operating on iOS, the user must configure their mobile device to share location information with applications capable of using that information. *Id. Third*, the user must affirmatively enable Location History in their Google Account. *Id.* ¶ 8. As of 2021, only approximately one-third of Google Account holders worldwide had opted in to Location History. *Id.* ¶ 12. *Fourth* and finally, for Google to save Location History information about where a particular user has been with their Location History–enabled mobile device, the user must power on their device, sign in to Google on their device, and then carry that device with them. *Id.* ¶ 8. *Only* when a user takes all of the steps detailed above is the resulting Location History data communicated to Google for processing and storage in association with the user's account. *Id.* ¶ 9.

[1] Location History information may be considerably more precise than other types of data, including cell-site location information ("CSLI"). While CSLI triangulates the location of a phone by assessing the phone's distance from nearby cell towers and using these distances to estimate the location of the device, Location History combines cell tower information with multiple other inputs to estimate distances. Location History can, in some instances, estimate a device's location to within approximately twenty meters or less. McGriff Decl. ¶ 11.

When a user enables Location History, the user can then visualize, chronicle, and curate locations they have visited while in possession of their compatible mobile devices, allowing them to reflect on travel and activities, and share that information with others. *Id.* ¶¶ 4, 5. *See* Fig. 1. Location History users can also access other benefits on their Google devices or applications. For instance, they can obtain personalized content or recommendations based on places they have visited. *Id.* ¶ 6.

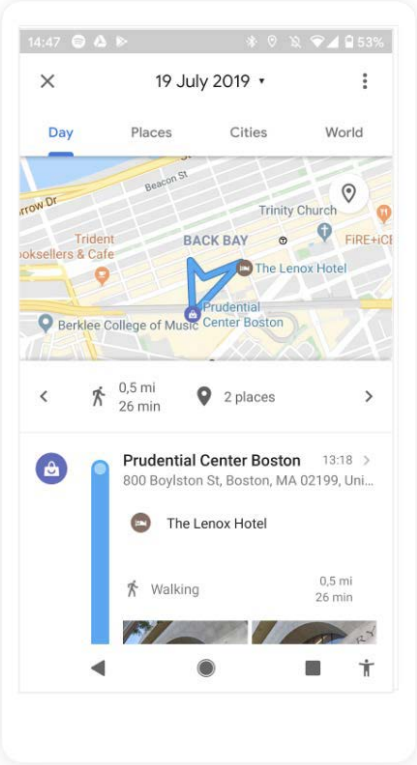


Figure 1. Sample Google Timeline.

Users retain complete control over their Location History data. Users can pause Location History at any time for their Google Account and for all devices or only certain devices.[2] They can also review, edit, and delete their Location History.[3] Users can delete their Location History in whole or in part—just as an email user can delete their entire email account or delete particular emails from their inbox. By deleting Timeline entries, a user also deletes the underlying Location History information.[4] When a user deletes data in their Google Account, Google immediately starts the process of removing it from the product and its systems.[5] Users can also choose to have Google *automatically* delete their Location History after 3, 18, or

[2] Google, Manage Your Location History, https://support.google.com/accounts/answer/3118687?hl=en (last visited July 5, 2022) ("You can pause Location History at any time in your Google Account's Activity controls.").
[3] Google, Google Maps Timeline, https://support.google.com/maps/answer/6258979?hl=en&co=GENIE.Platform%3DAndroid#zippy=%2Cchange-the-places-that-you-visited-activities-that-youve-done (last visited July 5, 2022) ("If a place is wrong on Timeline, you can edit the location and when you were there.").
[4] *Id.*
[5] *See* Google, Privacy & Terms, https://policies.google.com/technologies/retention (last visited July 5, 2022).

36 months. *Id.* ¶ 10.[6] For users who opted in to Location History after the summer of 2020, Location History is automatically deleted after 18 months by default; users can change that default setting by logging in to their Google Accounts.[7]

II. The Search Warrant

The Government has obtained a warrant seeking information about users whose Location History indicates their devices may have been within any of three specified geofences during the relevant search periods. The warrant indicates that the investigation relates to a violation of 18 U.S.C. § 1951, "Interference with Commerce by Threats or Violence," committed on April 14, 2022. Warrant, Attachment B.II, "Information to Be Seized." While Google does not have access to the affidavit supporting the warrant, it appears, based on the search areas and times, that the warrant relates to an armed robbery of a money courier service vehicle.[8]

While the warrant includes location coordinates and a defined search radius, the warrant does not include maps of the defined search areas, likely making it difficult for the Court to have appreciated from the face of the warrant application alone the expansive size of the geofences, the types of locations covered, and the vast amounts of places and people the search would sweep in.

Location 1 is a 300-meter radius around a central point proximate to a business named "Better Money Decisions" in Santa Fe, New Mexico (central point 35.6580480, -105.9503424), for a search period of Thursday, April 14, 2022, at 12:25 p.m. to 12:35 p.m. MDT (10 minutes).

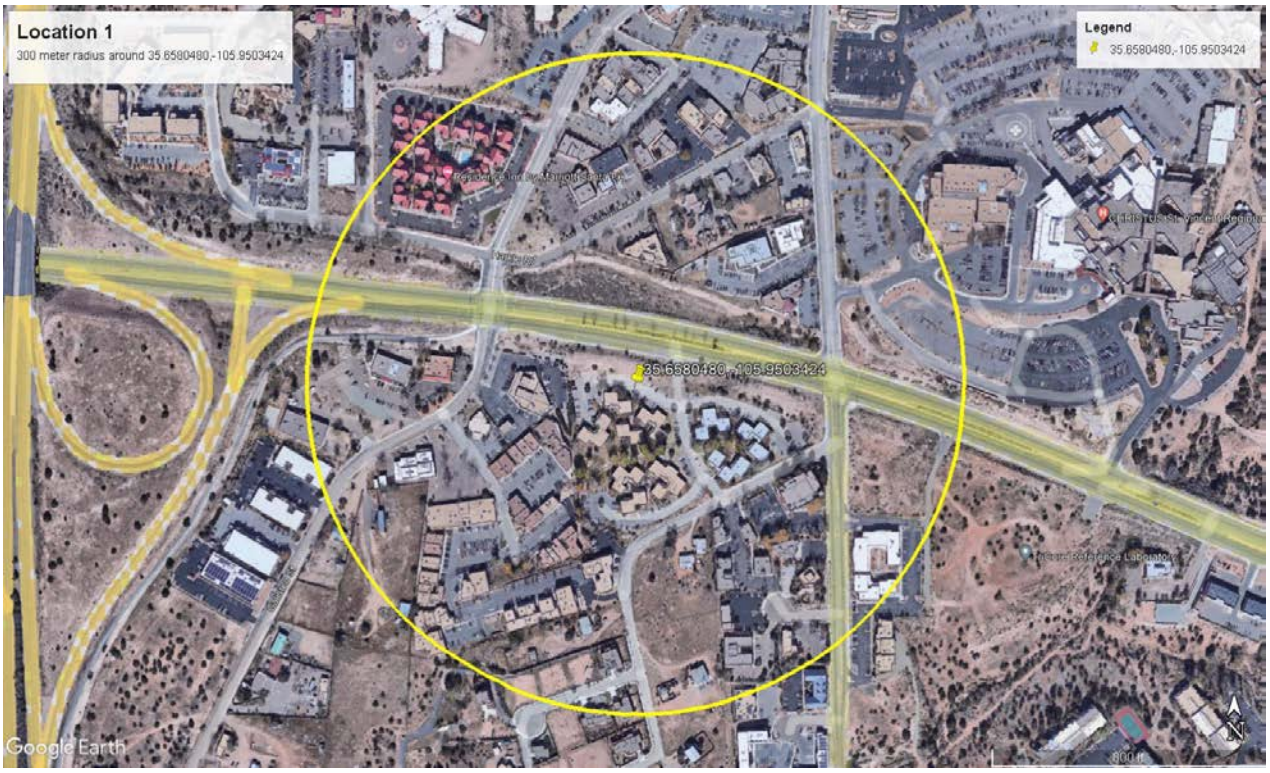
---

[6] *Supra* note 3 (providing instructions for users to enable automatic deletion of Location History that is older than 3 months, 18 months, or 36 months).

[7] Sundar Pichai, *Keeping your private information private*, Google Blog (June 24, 2020), https://www.blog.google/technology/safety-security/keeping-private-information-private/ ("Starting today, the first time you turn on Location History—which is off by default—your auto-delete option will be set to 18 months by default.").

[8] *One or more suspects sought in Santa Fe armed robbery*, Santa Fe New Mexican, (Apr. 17, 2022), https://www.santafenewmexican.com/news/local_news/one-or-more-suspects-sought-in-santa-fe-armed-robbery/article_594ed2b4-bda2-11ec-af96-1f14e0ecb0a7.html; Scott Brown, *Santa Fe money courier robbery suspect at large*, KRQE News (Apr. 16, 2022, 6:07 PM MDT), https://www.krqe.com/news/crime/santa-fe-money-courier-robbery-suspect-at-large/.

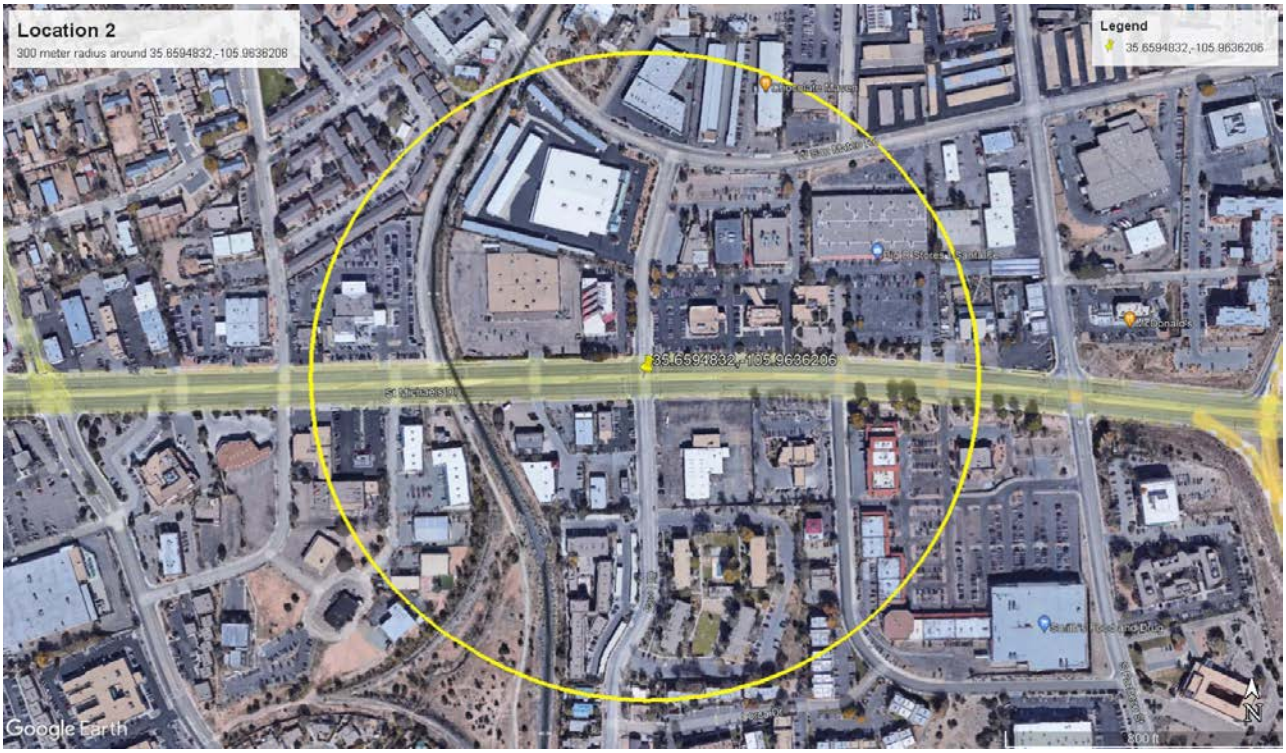
In addition to the financial services business, the geofence contains, among other things, approximately 20 individual medical offices, including a portion of an ob-gyn practice, a portion of the St. Vincent Regional Medical Center parking lot, and a portion of the St. Vincent Pediatrics building; at least three pharmacies; at least two law firms; the majority of the Residence Inn by Marriott Santa Fe; a portion of St. Michael's Drive, which handles approximately 25,000 to 30,000 vehicles per day;[9] a portion of the Highway 285 off-ramp; and banks, spas, and numerous other commercial businesses. Upon information and belief, this search area and time covers the suspected criminal activity.[10]



Location 2 is a 300-meter radius around a central point that falls on St. Michael's Drive in Santa Fe, New Mexico (central point 35.6594832, -105.9636206), for a search period of Thursday,

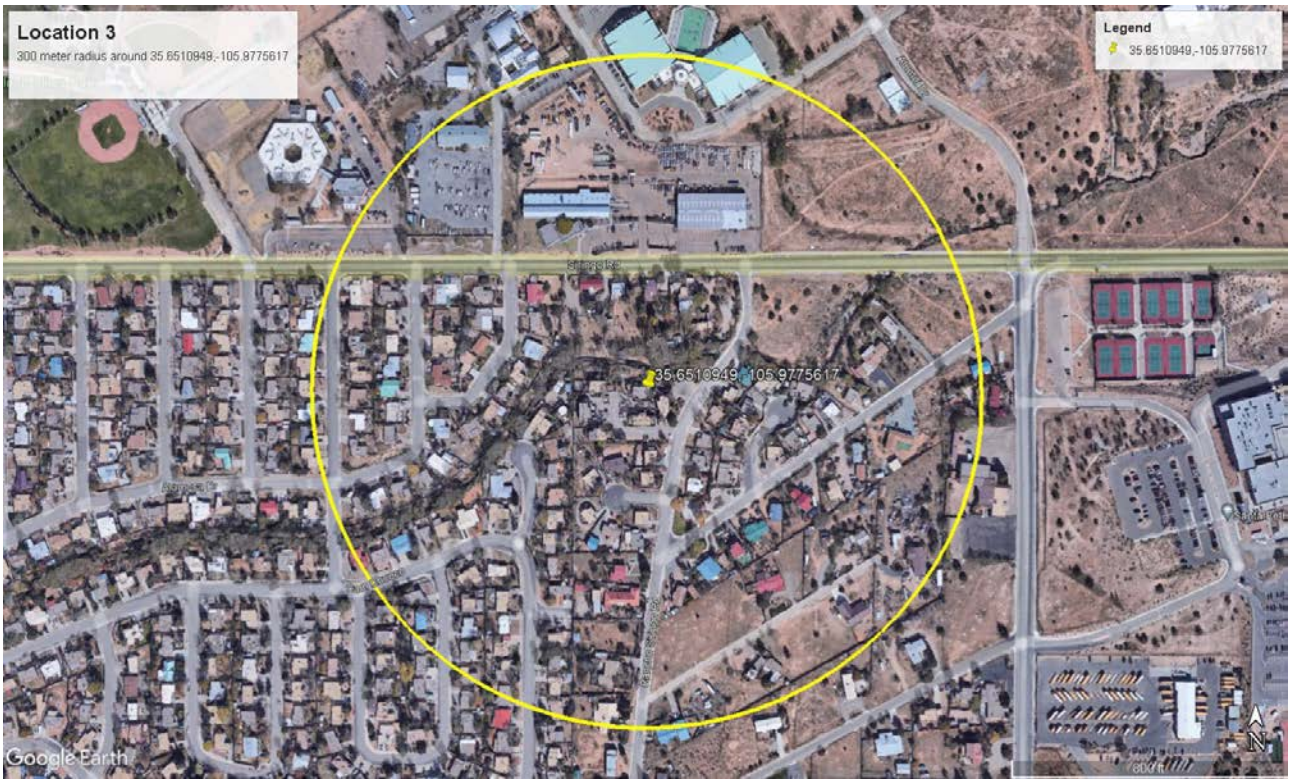
[9] City of Santa Fe, St. Michael's Boulevard, https://www.santafenm.gov/st_michaels_boulevard (last visited July 5, 2022).
[10] Santa Fe New Mexican, *supra* note 8 (indicating that an armed robbery occurred around 12:30 p.m. on April 14 in the area of the 400 block of St. Michael's Drive); Brown, *supra* note 8 (same).

April 14, 2022, at 12:15 p.m. to 12:25 p.m. MDT (10 minutes). The geofence contains, among other things, a church; two large apartment complexes; a portion of St. Michael's Drive; a large general store (Big R); an animal shelter; a branch office of the Department of Motor Vehicles; warehouses; a Starbucks and numerous restaurants (searched during the lunch hour); and numerous other commercial businesses, including a chocolate store, a consignment shop, a gym, a storage facility, and two gas stations.



Location 3 is a 300-meter radius around a central point that falls on an apartment complex, address 2110 Rancho Siringo Road, in Santa Fe, New Mexico (central point 35.6510949, -105.9775617), for a search period of Thursday, April 14, 2022, at 1:45 p.m. to 2:09 p.m. MDT (24 minutes). The geofence contains, among other things, a six-building apartment complex; more than 120 homes; multiple roads; a portion of a tennis and soccer facility and the entirety of its adjacent parking lot; the New Mexico State Surplus Property building and parking lot; the New Mexico State Printing and Graphics building and parking lot; the Santa Fe ITT

Department and parking lot; and the parking lot for Santa Fe Police Records. Upon information and belief, this search area covers the location of the suspect's abandoned vehicle, which was recovered by police on April 14 around 2:00 p.m. MDT.[11]



Together, the geofences encompass more than 200 acres of densely populated commercial and residential areas in Santa Fe:

[11] Santa Fe New Mexican, *supra* note 8 (indicating that the armed robbery suspect's vehicle was recovered around 2:00 p.m. on April 14 in the 2100 block of Rancho Siringo Road).

The warrant defines the property to be searched as Google "location history data . . . generated from devices and that reported a location within the geographical region bounded by the latitudinal and longitudinal coordinates, dates, and times" defined in the warrant (the "Initial Search Parameters") and "[i]dentifying information for Google Accounts associated with the responsive location history data." Warrant, Attachment A. The warrant defines "Items to be Seized and Searched" in two parts. Warrant, Attachment B. First, as to "Information to be disclosed by Google," the warrant directs the following process:

> (1) Google shall query location history [sic] data based on the Initial Search Parameters specified in Attachment A.
>
> (2) For each location point recorded within the Initial Search Parameters, Google shall produce to the government anonymized information specifying the corresponding unique device ID, timestamp, coordinates, display radius, and data source, if available (the "Anonymized List").
>
> (3) The government shall review the Anonymized List to remove devices, if any, that it can determine that are likely not relevant to the investigation (for example, devices moving through the Target Location in a manner inconsistent with the facts of the underlying case).

> (4) For the remaining device IDs, Google is required to provide to the government upon its request identifying information, as defined in 18 U.S.C. § 2703(c)(2), for the Google Account associated with each identified device ID.

Id., Attachment B.I. Second, as to "Information to Be Seized," the warrant authorizes seizure of:

> All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 1951 – "Interference with Commerce by Threats or Violence" that was committed on April 14, 2022 involving unknown person(s).

Id., Attachment B.II.

Nearly 450 devices were responsive to the search. Google has not produced any records and instead moves to quash the warrant. Google has conferred with the Government, and the Government has indicated it will oppose the present motion.[12]

ARGUMENT

The Fourth Amendment limits government power and protects individual privacy. It provides that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. Its "basic purpose" is "to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018) (citation omitted). It is well established that "any intrusion in the way of search or seizure is an evil, so that no intrusion at all is justified without a careful prior determination of necessity." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971), *holding modified by Horton v.*

[12] The Government asked whether Google would object to an amended warrant that drew narrower geofences around the target locations. Given the important Fourth Amendment issues at stake, Google believes it is important that this matter be brought before the Court to apprise the Court of the scope of the pending warrant and for the Court's consideration of the Fourth Amendment concerns the warrant raises.

California, 496 U.S. 128 (1990). The warrant requirement protects against this evil by eliminating searches not based upon probable cause and requiring the place to be searched and the items to be seized to be described with particularity, thus preventing the government from engaging in "a general, exploratory rummaging in a person's belongings." *Id.*

Yet the warrant here would allow the Government to engage in a modern-day exploratory search of data reflecting the detailed location and movements of *hundreds* of individuals. The search touches upon the most intimate and protected private places of citizens—their homes and their devices. *See Kyllo v. United States*, 533 U.S. 27, 31 (2001); *Riley v. California*, 573 U.S. 373, 395 (2014). The wide net cast by the Government would track Location History users, by way of their devices, into highly sensitive, personal, and potentially even confidential spaces, including doctor's offices, pharmacies, lawyer's offices, and churches.

As set forth more fully below, the Court should quash the warrant for at least three independent and sufficient reasons. First, the warrant is overbroad because the scope of the search exceeds what is justified by the evidence sought. Second, the warrant, which authorizes the Government to seek identifying information about those devices that it deems "relevant" to the investigation, grants unfettered discretion to the executing officers and, therefore, lacks particularity. Third, while Google does not have access to the affidavit supporting the warrant, it is unlikely, given the nature of the Location History service, that the Government has established a reasonable basis for the Court to find probable cause to believe that evidence of the crime will be found in Location History.

I. The Warrant, Which Authorizes the Government to Review the Private Location Data of Hundreds of Users in a Search for a Single Suspect, Is Overbroad

The Fourth Amendment requires warrants to "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The "manifest purpose"

of the particularity requirement is to prevent general searches. *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). The authorization to search is thereby limited "to the specific areas and things for which there is probable cause to search," thus ensuring that the search "will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Id.*; *Carpenter*, 138 S. Ct. at 2213. Consequently, a warrant with an "indiscriminate sweep" is "constitutionally intolerable," and any warrant that is overly broad is invalid. *Stanford v. Texas*, 379 U.S. 476, 486 (1965).

The Department of Justice has recently emphasized the Government's rigorous adherence to these requirements in the context of search warrants issued pursuant to the Stored Communications Act, such as the warrant before the Court. U.S. Dep't of Justice, White Paper, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act* (Apr. 2019), https://www.justice.gov/opa/press-release/file/1153446/download (hereinafter "DOJ Cloud Act White Paper"). Describing the requirements for obtaining a warrant for electronic communications as "perhaps the toughest in the world" and "highly protective of individual privacy," the Government highlighted that all such warrants "must describe with particularity the data to be searched and seized; fishing expeditions to see if evidence exists are not permitted." *Id.* at 8.

Thus, the Fourth Amendment mandates that if the Government can establish probable cause to believe that evidence of the crime is likely to be found in Location History, its search of Location History must be cabined to the places where evidence is likely to be found and its seizure to those things likely to constitute evidence. *Coolidge*, 403 U.S. at 467 ("[T]hose searches deemed necessary should be as limited as possible."). But the warrant is not so circumscribed. The Government has instead sought approval to conduct an exploratory search over large, densely

populated residential and commercial areas in Santa Fe. The more than 200 acres searched include large stretches of land where, upon information and belief, the Government has no reason to believe the suspect may have been. The warrant permits the Government to indiscriminately seize all Location History data responsive to the broad search so that it may then sift through that data "to see if evidence exists." DOJ Cloud Act White Paper at 8. The warrant is, therefore, overbroad. *Cf. People v. Gutierrez*, 222 P.3d 925, 940 (Colo. 2009) (warrant authorizing seizure of all tax returns for two-year period from a tax service business was invalid where the supporting affidavit merely speculated that some unknown number of the business's 5,000 clients had committed, or were committing, crimes); *United States v. Abrams*, 615 F.2d 541, 545 (1st Cir. 1980) (in the context of a Medicare fraud investigation, warrant was invalid where it authorized "an indiscriminate seizure" of records from three doctor's offices); *United States v. Ellis*, 971 F.2d 701, 706 n.7 (11th Cir. 1992) (a general search is one that creates a "danger of invading the privacy of a person under no suspicion at all, or of searching an entire neighborhood").

Specifically, the warrant directs Google to produce and the Government to seize Location History data for any users whose stored Location History indicates they may have been within the search areas, which encompass more than 200 acres, during the search periods, which total 44 minutes. The warrant authorizes the Government to seize the Location History and identifying information of individuals who may have been:

- Sitting within the privacy of their homes (Locations 2 and 3);
- Taking their sick child to the doctor's office (Location 1);
- Attending a doctor's appointment (Location 1);
- Consulting with their lawyer (Location 1);
- Praying in church (Location 2);
- Driving along one of the busiest roads in Santa Fe during the middle of the afternoon (Locations 1 and 2); or

- Enjoying the comfort of their hotel (Location 1).

The search areas stretch 300 meters—*more than the length of three football fields*—in all directions from the central coordinates. Assuming the central coordinates correspond to the area where the suspect is believed to have been, the search extends well beyond any areas where there is probable cause to believe evidence of the crime may be located. For example, the central coordinates for Location 1 appear to correspond to the area where the crime occurred.[13] The central coordinates for Location 3 appear to correspond to the area where the suspect's vehicle was recovered.[14] Google speculates, based on area and time, that the central coordinates for Location 2, the center of St. Michael's Drive, are designed to detect the suspect's device as the suspect traveled along that road on the way to the site of the crime. Assuming Google has accurately identified the crime under investigation, the Government can pinpoint with near precision the locations and times the suspect was within Locations 1 and 3, but the warrant authorizes a search that is vastly more expansive, unnecessarily authorizing the Government to review the private location data of hundreds of users who have nothing to do with the crime under investigation. Because the warrant fails to "ensure that the search is confined in scope" to those areas the Government has established probable cause to search, it is overbroad. *Cassady v. Goering*, 567 F.3d 628, 636 (10th Cir. 2009) (warrant overbroad where it contained no limitation on the scope of the search and was "not as particular as the circumstances would allow or require" (internal quotation marks and citations omitted)).[15]

[13] Santa Fe New Mexican, *supra* note 8 (indicating that an armed robbery occurred around 12:30 p.m. on April 14 in the area of the 400 block of St. Michael's Drive); Brown, *supra* note 8 (same).

[14] Santa Fe New Mexican, *supra* note 8 (indicating that the armed robbery suspect's vehicle was recovered around 2:00 p.m. on April 14 in the 2100 block of Rancho Siringo Road).

[15] If Google's speculation about the crime under investigation is not accurate, then this would alter the precise outline of the *ways* in which the warrant is overbroad, but not the determination of overbreadth itself. It is difficult to imagine a scenario in which the Government could establish probable cause to search for the identities of all users whose saved Location History indicates they may have been within 200+ acres of Santa Fe.

Developing geofence case law strongly supports the conclusion that the warrant is overbroad. Google is aware of seven published opinions addressing the lawfulness of geofence warrants. Most recently, the U.S. District Court for the Eastern District of Virginia had cause to address a geofence warrant in the context of a motion to suppress. *United States v. Chatrie*, No. 19cr130, 2022 WL 628905, at *11 (E.D. Va. Mar. 3, 2022). The subject warrant was issued in association with a bank robbery investigation and included a single geofence that spanned a 150-meter radius "in an urban environment." *Id.* The search area included a bank and a nearby church, and the search period spanned an hour during the time of the robbery. *Id.* The search yielded 19 responsive devices. *Id.* at *13. The court held that the warrant was invalid because it was unsupported by probable cause, lacked particularity, and was overbroad. As to the last finding, the court noted that "it [was] difficult to overstate the breadth of [the] warrant, particularly in light of the narrowness of the Government's probable cause showing," which relied largely on the mere fact that "the perpetrator 'had a cell phone in his right hand and appeared to be speaking with someone on the device.'" *Id.* at *21. The court declined to suppress the geofence records under the good faith exception, but it nonetheless "strongly caution[ed] that this exception may not carry the day in the future." *Id.* at *30.

The remaining six published geofence opinions address the government's application for issuance of a geofence warrant. Of the six, four courts rejected the government's geofence warrant application on the basis that the proposed search lacked probable cause and particularity and suffered from overbreadth. *See, e.g.*, *Matter of the Search of Info. that is Stored at the Premises Controlled by Google LLC* ("*D. Kansas Geofence Warrant Application*"), 542 F. Supp. 3d 1153, 1158 (D. Kan. 2021) (denying geofence warrant application for lack of probable cause and concerns over particularity and overbreadth, including that "the geofence boundary appears to

potentially include the data for cell phone users having nothing to do with the alleged criminal activity"); *Matter of Search of Info. Stored at Premises Controlled by Google* ("*Pharma II*"), 481 F. Supp. 3d 730, 756 (N.D. Ill. 2020) (denying geofence warrant application for lack of probable cause and particularity and overbreadth, and holding that particularity is lacking where the government is permitted "to sort through" results "to identify the suspect by process of elimination"); *Matter of Search of Info. Stored at Premises Controlled by Google, as further described in Attachment A* ("*Pharma I*"), No. 20 M 297, 2020 WL 5491763, at *1 (N.D. Ill. July 8, 2020) (denying geofence warrant application for overbreadth and lack of particularity where the government sought data related to geofences in densely populated areas for 45-minute intervals); *In re Search of Info. Stored at the Premises Controlled by Google* ("*Virginia Hotel Geofence Warrant Application*"), No. KM-2022-79, 2022 Va. Cir. LEXIS 12* (Va. Cir. Ct. Feb. 24, 2022) (denying geofence warrant application for lack of probable cause and particularity and overbreadth where the government sought data related to geofences over a motel and adjoining spaces).

The two courts that have issued written opinions granting geofence warrant applications did so only where the geofences and search periods were tailored to strictly minimize impact on individuals unrelated to the criminal activity. The first granted the government's geofence warrant application where the six geofences were narrowly "constructed to focus on the arson sites and the streets leading to and from those sites" and where target time periods, which totaled 24 minutes, 17 minutes, 15 minutes, 16 minutes, 37 minutes, and 31 minutes, were "in the early hours of the morning when [the subject] commercial businesses [were] usually closed and unoccupied" such that "location data from uninvolved individuals [would] be minimized." *Matter of Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation* ("*Arson*"), 497 F. Supp. 3d 345, 358 (N.D. Ill. 2020). The government provided the court with

detailed information, sourced from interviews and video surveillance, to satisfy the court that "the scope of the warrant would not result in the collection of a broad sweep of data from uninvolved individuals for which there is no probable cause." *Id.* at 359. In granting the warrant application, the court acknowledged that, because geofence warrants target *locations* and not *individuals*, "it is easy for a geofence warrant, if cast too broadly, to cross the threshold into unconstitutionality because of a lack of probable cause and particularity, and overbreadth concerns under Fourth Amendment jurisprudence." *Id.* at 353.

The second granted the government's geofence warrant application where the search was cabined to those precise, narrowly drawn locations and times the government knew the suspects to be based on CCTV footage, and where that footage showed the suspects speaking on cell phones. *Matter of Search of Info. Stored at Premises Controlled by Google LLC* ("*DDC Geofence Warrant*"), No. 21-SC-3217, 2021 WL 6196136, at *5, *13 (D.D.C. Dec. 30, 2021). CCTV footage indicated that the suspects were either alone in the geofences during the search periods or, at most, two to three other individuals were in the geofence with the suspects. *Id.* The eight search periods authorized by the warrant ranged from 2 to 27 minutes each. *Id.*[16]

In stark contrast to the geofence warrants approved by the *Arson* and *DDC Geofence Warrant* courts, the geofences in the present warrant are not tailored in area or shape to cover the location of suspected criminal activity while excluding individuals unrelated to the criminal activity. Instead, the Government has drawn large, circular geofences over more than 200 acres of densely populated Santa Fe to be searched during the middle of the day when covered structures

[16] These cases incorrectly conclude based on inaccurate factual statements in the government's supporting affidavits that, given the pervasiveness of cell phones and of the Android operating system and Google mobile applications, it is likely that evidence of the crime—namely, the suspect's identity—will be found within data responsive to a geofence search. But, as detailed above in Background, Section I.B, Location History is not synonymous with device-level location services on either Android or iOS. It is, therefore, *not* the case that most individuals within the geofence will be identified by a geofence search.

and roads are likely to be occupied. Notably, the warrant is significantly broader than the warrant held to be invalid in *Chatrie*, which involved a one-hour search of a 150-meter radius geofence that included a bank and a church. It is also significantly broader than geofence warrant applications rejected by other courts on Fourth Amendment grounds:

Matter	Total Search Area	Total Search Period	Holding
United States v. Chatrie	17.5 acres in an urban environment.	1 hour	Unconstitutional
Virginia Hotel Geofence Warrant Application	Almost the entirety of a motel's property, including the motel, its parking lots, and adjoining property owned by the motel.	Nearly 3 hours	Unconstitutional
D. Kansas Geofence Warrant Application	A "sizeable business establishment."	1 hour	Unconstitutional
Pharma I	Two 100-meter radius geofences, covering over 15 acres of land, which included medical offices, a large residential complex, restaurants, and various businesses. The warrant application proposed two separate search periods for the second geofence.	2 hours and 15 minutes	Unconstitutional
Pharma II	Two polygons, each drawn over a separate business. Included in the search areas were residential units above one of the businesses, a sidewalk, a portion of the streets on which the businesses were situated, and the parking lot adjacent to one of the businesses. The warrant application proposed two separate search periods for the second location.	2 hours and 15 minutes	Unconstitutional

Matter	Total Search Area	Total Search Period	Holding
Arson	Four geofences that were carefully constructed to focus on the subject arson sites and the streets leading to and from those sites, and to exclude residences and other commercial buildings in the vicinity. Two of the four geofences included two search periods.	2 hours and 19 minutes in a commercial area in the early morning hours	Warrant application granted
DDC Geofence Warrant	0.20 acres (or 875 square meters), which included the front half of a business and its parking lot, searched for eight separate search periods.	3 hours and 5 minutes	Warrant application granted
The Subject Warrant	Over 200 acres covering densely populated residential and commercial areas, and including more than 100 homes, more than 20 doctor's offices, a church, busy roadways, a hotel, and numerous businesses.	44 minutes during the middle of the afternoon	

The warrant, which would reveal to the Government the location and identity of nearly 450 "private citizens who [have] no reason to incur Government scrutiny," is overbroad and must be quashed. *Chatrie*, 2022 WL 628905, at *21.

II. The Warrant, Which Grants the Government Unfettered Discretion to Determine What Data to Seize, Lacks Particularity

To safeguard against exploratory, general searches, the Fourth Amendment requires warrants to "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. A warrant is sufficiently particular when, "[a]s to what is to be taken, nothing is left to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 196 (1927). The particularity requirement is especially critical in the context of a digital search because the government's ease of access to vast amounts of personal data increases the risk that it may conduct wide-ranging searches into individuals' private affairs. *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009). That is certainly the case here.

The warrant authorizes multiple independent investigative steps. First, it requires Google to produce de-identified device information for devices responsive to the search. Then, it authorizes the Government, with no judicial oversight and based on its unilateral determination that certain devices and associated accounts are "relevant to the investigation," to require Google to produce identifying information regarding those accounts. Warrant, Attachment B.I. The warrant therefore grants the Government *unbridled discretion* to seize more intrusive and personal data about users implicated by the search. It contains no limiting principles or "objective guardrails by which officers could determine which accounts would be subject to further scrutiny." *Chatrie*, 2022 WL 628905, at *25 (emphasis omitted); *see also Pharma II*, 481 F. Supp. 3d at 754 (invalidating geofence warrant that "put[] no limit on the government's discretion to select the device IDs from which it may then derive identifying subscriber information from among the anonymized list of Google-connected devices that traversed the geofences"). By authorizing multiple, independent investigative steps without scrutiny by a detached and neutral magistrate over each, the warrant permits the Government to determine whose privacy to infringe upon and whether that infringement is reasonable, decisions reserved by the Fourth Amendment to a court.[17]

[17] The warrant is insufficiently particular for the additional reason that it defines the items to be seized as "evidence of violations of 18 U.S.C. § 1951 – 'Interference with Commerce by Threats or Violence' that was committed on April 14, 2022 involving unknown person(s)." Warrant, Attachment B.II ("Information to Be Seized"). But the warrant does not specify any specific features or limiting principles to inform *how* the Government is to differentiate devices considered "evidence" of the listed crimes from the thousands of other devices responsive to the search. *See, e.g.*, *United States v. Leary*, 846 F.2d 592, 601–02 (10th Cir. 1988) (warrant invalid where it broadly permitted seizure of documents relating to "the purchase, sale and illegal exportation of materials in violation of the federal export laws," and citing cases supporting the conclusion that "reference to a broad federal statute is not a sufficient limitation on a search warrant"). The lack of any specific description of items the Government is authorized to seize is especially problematic because any "evidence" within the responsive Location History will otherwise be largely indistinguishable from all of the other Location History records produced by Google pursuant to the warrant. *See United States v. Fuccillo*, 808 F.2d 173, 176–77 (1st Cir. 1987) (warrants to search a fashion distributor, a warehouse, and a retail clothing store for "cartons of women's clothing" that constituted evidence of a violation of 18 U.S.C. § 659, Possession of Goods Stolen from Interstate Shipments, were insufficiently particular because they lacked any "physical criteria or detailed description" that might "enable [the executing officers] to determine what they might lawfully seize," thus permitting the agents "to search, and seize, indiscriminately" (cleaned up)). Instead, the warrant permits the Government to sort through all responsive data in the hopes that it might identify a suspect "by process of elimination." *Pharma II*, 481 F. Supp. 3d at 756. This is precisely the type of exploratory search the warrant requirement was intended to prevent.

Because the warrant is insufficiently particular, it must be quashed.

III. The Warrant Lacks Probable Cause

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause." U.S. Const. amend. IV. The probable cause standard is objective and requires the Government to present facts that "would warrant a person of reasonable caution in the belief that contraband or evidence of a crime is present." *Florida v. Harris*, 568 U.S. 237, 243 (2013) (cleaned up). While probable cause does not require certainty, mere belief and speculation is not sufficient. *Brinegar v. United States*, 338 U.S. 160, 175 (1949).

Google does not have access to the Government's affidavit supporting the warrant, but it is difficult to imagine that the Government has established probable cause to support the search. To establish probable cause to believe that evidence of the crime will be found in Location History, the Government must present a sufficient basis for a person of reasonable caution to believe all of the following:

1) The suspect is a cell phone user;
2) The suspect had a cell phone on their person while located within geofences during the search periods;
3) The suspect is also a Google Account holder;
4) The suspect has also opted in to Google's Location History service;
5) The suspect had powered the device on; and
6) The suspect had signed in to their Google Account on that device.

Regardless, the Government will have seized all responsive Location History at the moment when Google produces the data and the Government takes possession of the same. *See, e.g.*, *United States v. Ganias*, 755 F.3d 125, 137 (2d Cir. 2014) (holding that the government's retention of electronic copies of the defendant's personal computer "deprived him of exclusive control over those files," which "constituted a seizure within the meaning of the Fourth Amendment"), *vacated by United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016) (en banc). Thus, the warrant authorizes a seizure that is limited only by the place searched and without *any* reference to criminal activity or other limiting factors. The "seizure" authorized in Attachment B of the warrant may be more appropriately characterized as an independent investigative step allowing the Government to take possession of and review additional personal data of nearly 450 Google users.

Assuming the Government does not have direct evidence establishing that each of these conditions has been fulfilled, then it is the compound probability that *all* of these conditions will be fulfilled—not just that *any one* of these conditions will be fulfilled—that underpins the Government's attempted basis for probable cause.

The affiant may speculate, based on their knowledge and experience, that the suspect carried a cell phone during the commission of the crime. That speculation alone, without supporting statements establishing a reasonable basis to believe that this suspect in particular is likely to have carried a cell phone, would be an insufficient basis to establish probable cause to believe that evidence of the crime will be found within a specified individual's cell phone—let alone Location History. *See, e.g.*, *United States v. Griffith*, 867 F.3d 1265, 1272 (D.C. Cir. 2017) (warrant to search defendant's house for a cell phone was not supported by probable cause where the government speculated that the defendant was a cell phone user; while the court "[did] not doubt that most people today own a cell phone," probable cause required a reason to think that the defendant "in particular" owned a cell phone). For example, news articles about the crime that Google believes to be the subject of the investigation indicate that a single suspect was involved and provide a description of a single suspect based on eyewitness statements.[18] While the stories state that "one or more" individuals may have been involved, no details are provided about a second suspect having been sighted by any witnesses. If there is no evidence that the suspect was working and communicating with an accomplice, then it may be equally plausible that the suspect

[18] Santa Fe New Mexican, *supra* note 8 ("Santa Fe police seek help finding one or more men who robbed a money courier service vehicle Thursday, according to a news release. . . . Witnesses described the man as in his mid-20s and about 5 feet, 10 inches, with a thin build and wearing a dark jacket and a mask. He was seen fleeing in a dark-colored Toyota Camry that had been stolen around 10:30 a.m., and officers recovered the car about 2 p.m. in the 2100 block of Rancho Siringo Road."); Brown, *supra* note 8 ("Santa Fe police are looking for a man who they say robbed a money courier service vehicle on Thursday around 12:30 p.m;" the man is described as "being in his mid-20s, Hispanic, around 5'10" [sic] tall with a thin build.").

did not have a cell phone on his person in an attempt to evade detection as it would be that he carried one with him during commission of the crime.

But even if the Government has offered evidence that the suspect carried a cell phone within the geofences during the search periods (based upon, for example, video surveillance or eyewitness statements), that, too, would be an insufficient basis to support a reasonable belief that the suspect was also a Google Account holder who had affirmatively opted in to Location History and taken all requisite steps for Location History "within" the geofences to be saved. Unless the Government has offered facts to support a reasonable belief that the suspect was a Location History user, a search of Location History would be based on nothing more than hope that reviewing the Location History data of more than 450 users might provide a key piece of evidence that the Government has otherwise been unable to obtain. But probable cause requires more than speculation, and the Government is not entitled to engage in exploratory searches simply because it has no other targeted options available to it. *Cf. In re Applications of the United States of Am. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 206 F. Supp. 3d 454, 457 (D.D.C. 2016) (holding, in the context of an application for an order pursuant to § 2703(d), that the government is not entitled to the disclosure of *more* data simply because it knows the least).

Critically, statistics regarding the prevalence of cell phones—among the general population or among individuals engaged in criminal activities—coupled with statistics regarding the prevalence of the Android, iOS, and Google's mobile applications, such as Google Maps, are insufficient to establish probable cause to search Location History because Location History is not synonymous with device-level location services on either Android or iOS or with Google mobile applications, and whether a user has their device location permission enabled, let alone a precise location permission for any app, is wholly independent of such statistics or a user's choice to opt-

in to Location History. It is therefore *not* the case, for example, that an individual who has merely signed in to a Google Account or used a Google application on their cellular device will save Location History to their account. Nor is it the case that an individual who merely engages with a Google application on their device, such as allowing Google Maps to access their location and navigating via Google Maps, will concurrently save Location History to their account. Location History may be saved in those circumstances—but only when the user has also taken the requisite steps to enable Location History to be collected from the relevant device. *See* Background, Section I.B, *supra*.[19]

If the Government's statement of probable cause is based on a similar formulation—i.e., criminals engaged in robberies often use cell phones and many cell phone users are Google Account holders who sign into and use Google services on their devices—then the Government has failed to establish a sufficient basis for a reasonable person to believe that the suspect's identity will be found in Location History. Indeed, this kind of vague and generic support for searching a large trove of personal, detailed location data obtained from a cellular device could apply "in any case involving criminal conduct by a person (or persons) with [a cell phone]—which includes almost everyone at this point." *In re Applications of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d)*, 206 F. Supp. 3d at 458; *see also Chatrie*, 2022 WL 628905, at *20–21 (geofence warrant that sought information about "*all* Google account owners who entered [a] geofence over the span of an hour" failed to establish probable cause that was particularized with respect to each person to be searched or seized); *Pharma II*, 481 F. Supp. 3d 730 (denying

[19] It is worth emphasizing, for the avoidance of doubt, that written opinions addressing geofence warrants have inaccurately described the nature of Location History and have based their probable cause analyses on inaccurate facts. *See* note 15, *supra*.

geofence application for lack of probable cause and particularity and holding that probable cause must be established for every individual within the geofence).

Courts have similarly found probable cause lacking in the context of physical searches where supporting affidavits failed to establish a direct connection between the place to be searched and evidence of the crime under investigation. *Griffith*, 867 F.3d at 1271 (warrant affidavit failed to establish that even if the defendant had a cell phone, it was likely to be found in his home); *United States v. Roach*, 582 F.3d 1192, 1202 (10th Cir. 2009) (warrant affidavit failed to provide sufficient basis for magistrate to find the requisite nexus between the listed address and the defendant where the affidavit did not specify the method used by agents to verify the defendant's place of residence).

Finally, probable cause cannot be established based on the fact that individuals responsive to the search will have been near the criminal activity under investigation because mere proximity to a crime does not establish probable cause. *See Ybarra v. Illinois*, 444 U.S. 85, 86 (1979) (warrant authorizing search of tavern and bartender for narcotics did not extend to patrons); *Pharma II*, 481 F. Supp. 3d at 753 (rejecting geofence warrant application that would have granted the government discretion to search for users who "traversed the geofences" based solely on those users' propinquity to the suspected criminal activity). Even if proximity were a sufficient basis for probable cause, because the search areas are so large, many—if not most—of the nearly 450 users swept into the search will not have been proximate to the suspected criminal activity in any event. *See, e.g.*, *Chatrie*, 2022 WL 628905, at *21 (geofence warrant did not meet Fourth Amendment reasonableness standard where the geofence was so large that it swept in users who may not have been "*remotely* close" to the crime scene).

CONCLUSION

For the reasons set forth above, Google respectfully requests that the warrant be quashed in its entirety.

WIGGINS, WILLIAMS & WIGGINS
A Professional Corporation

Electronically Filed

By *__/s/ Lorna M. Wiggins__*
Lorna M. Wiggins
1803 Rio Grande Blvd., N.W. (87104)
P.O. Box 1308
Albuquerque, New Mexico 87103-1308
(505) 764-8400
lwiggins@wwwlaw.us

Todd M. Hinnen
THinnen@perkinscoie.com
Pro hac vice pending
Hayley L. Berlin
HBerlin@perkinscoie.com
Pro hac vice pending
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101-3099
Telephone: 206.359.8000
Facsimile: 206.359.9000

Attorneys for Google LLC

We hereby certify that a copy
of the foregoing and the Declaration of
Marlo McGriff in Support of Motion
to Quash were emailed to Jack
Burkhead at Jack.E.Burkhead@usdoj.gov
on this 8th day of July, 2022.

WIGGINS, WILLIAMS & WIGGINS, P.C.

By *__/s/ Lorna M. Wiggins__*
Lorna M. Wiggins